Theoretical Computer Science 39 (1985) 207-224
North-Holland

REDUCTIONS AMONG POLYNOMIAL ISOMORPHISM TYPES*

Stephen R. MAHANEY**

AT&T Bell Laboratories, Murray Hill, NJ 07974, U.S.A.

Paul YOUNG***

Computer Science Department, FR-35, University of Washington, Seattle, WA 98105, U.S.A.

Communicated by R.V. Book
Received October 1983
Revised October 1984

Abstract. A set A is polynomial many-one reducible to a set B (A is Karp-reducible to B) if there is a polynomially computable function f such that, for all x, $x \in A$ iff $f(x) \in B$. Arbitrary sets A and B are of the same polynomial many-one degree if each is polynomial many-one reducible to the other. A and B are (polynomially) isomorphic if the function f can be taken one-to-one, onto, and polynomially invertible.

In classical recursive function theory, all many-one complete sets are recursively isomorphic. Berman and Hartmanis have observed that all known NP-complete sets are polynomially isomorphic, and have conjectured that all NP-complete sets (complete under Karp-reducibility) are isomorphic.

In this paper we show that not just the complete degree, but *every* polynomial many-one degree consists either of a single isomorphism type or else contains infinitely many isomorphism types densely ordered under one-one, size-increasing, polynomially invertible reductions and also contains infinitely many isomorphism types which are incomparable under one-one invertible reductions. In fact, we show that every countable partial ordering can be embedded in any such many-one degree. We also exhibit polynomial degrees which have infinitely many isomorphism types. No examples are known of degrees consisting of a single isomorphism type.

Keywords. Polynomial reduction, isomorphism, NP-complete set.

1. Introduction

In [1] it was shown that all known examples of NP-complete sets were polynomially isomorphic, and it was conjectured that all NP-complete sets are polynomially

* Some of the results given here were originally presented at the *1981 IEEE Foundations of Computer Science Conference* [17]. The remaining results were presented as part of a talk at a session of invited papers on Computational Complexity at the *1982 Summer AMS Meetings* [25], and also as one section of [26].

** Part of this work was done while the first author was at The Pennsylvania State University during 1980-1981.

*** Supported by NSF Research Grant MCS 7609212A, Purdue University, by the Division of Computer Science, University of California, Berkeley, as Visiting Professor during the 1982-83 academic year, and by NSF Grant MCS 7609212A, University of Washington.

isomorphic.[1] The conjecture, of course, implies that $P \neq NP$. In [17] it was shown that the many one-degree consisting of the NP-complete sets is either a single polynomial isomorphism type or else contains infinitely many isomorphism types with an ordering of type $\omega + 1$ under one-one, size-increasing, and invertible polynomial time reductions. The proofs used information about polynomial time padding functions and the technique of 'delayed diagonalization', and they applied to any polynomial many-one degree. It was conjectured in [17] that the proof techniques used there could be extended to yield incomparable isomorphism types and dense linear orderings of isomorphism types.

In [23], the corresponding question for all recursively enumerable degrees had been answered affirmatively. The proofs were entirely structural, with no diagonalizations required. The basic result stated in [23] was that "every nonrecursive many-one degree either consists of a single one-one degree or else contains a collection of one-one degrees which has, under one-one reducibility, the order type of the rationals".

In this paper we answer the above two conjectures of [17] by proving that every polynomial many-one degree either consists of a single polynomial isomorphism type or else contains a collection of isomorphism types which has, under one-one, size-increasing, polynomially invertible reductions, the order type of the rationals. We also prove that any such many-one degree contains infinitely many pairwise incomparable isomorphism types. In fact, we show that the isomorphism types of such a many-one degree form a *universal countable partial order* in that any countable partial order can be embedded in it. This is a powerful characterization since the existence in both directions of one-one size increasing and invertible reductions between two sets implies that the sets are isomorphic. However, since it is possible that the embedding may be extendible, it is not a complete characterization. For example, there conceivably could be minimal elements in certain degrees and no minimal elements in others.

We also exhibit degrees (the degree P and others constructed by delayed diagonalization [3, 13]) which have infinitely many isomorphism types. We know of no polynomial degrees which have a single isomorphism type.

The proofs given here are, in several ways, including their use of delayed diagonalization, based on those of [17]. On the other hand, the systematic use of polynomial structures, including polynomial cylinders and non-immunity of sets, uses the ideas of [23]. This allows us to also give a stronger treatment of *finite difference properties* in Section 4 of this paper, and it is this insight which allows us to obtain proofs which are more easily generalized than those of [17]. Once this

[1] In [25, 26, 10], new examples of structurally defined NP-complete sets are given for which there are no known proofs of polynomial isomorphism. The isomorphism problem for these new NP-complete sets is shown to be connected to the existence of polynomially computable 'trap-door' functions, and it is conjectured that these new NP-complete sets are all polynomially isomorphic only if polynomial trap-door functions do not exist, a supposition which is widely believed to be false.

appropriate *structural material* is developed, these more general proofs are actually simpler than those of [17].[2]

We stress that the results given here apply not just to the degree of the NP-complete sets, but to arbitrary degrees. For example, since it is known that not all sets in P are polynomially isomorphic (since one can construct sparse sets in P) it follows from our results that the polynomial degree consisting of the nontrivial elements in P splits into a universal countable partial order under suitable polynomial one-one reductions.

Similarly, the isomorphism question for the sets complete for the class of all r.e. sets under *polynomially computable functional reductions* is discussed in [4]. It is shown there that if an r.e. set is complete under polynomial time many-one reductions, then it is complete under one-one polynomial time reductions. On the other hand, the *natural creative sets* of [7] are explicitly defined using sufficiently restrictive reductions to make them all polynomially isomorphic. Strengthening the results of [4] by showing that the complete sets considered there are complete even under polynomial-time *invertible* reductions would then show that Dowd's complete sets are all polynomially isomorphic and hence the same as Hartmanis's natural creative sets. On the other hand, if Dowd's sets are not complete under invertible reductions, then our results show that his r.e. complete sets split into a universal countable partial order.

2. Cylinders and immune sets

A cylinder is a set which is isomorphic to $B \times \mathbb{N}$ for some set B.[3] Cylinders have played an important role for classification of r.e. sets in classical recursion function theory. Facts about cylinders may be found in [21]. A succinct summary of elementary facts about computable cylinders and a partial list of references may also be found in [23]. Polynomial cylinders were first used, at least implicitly, by Hartmanis, Baker, and Berman [2, 1, 6, 7]. They are perhaps first developed explicitly by Dowd [4].

The importance of cylinders is underscored by noting that all the known *natural* complete sets, such as SAT for NP and QBF for PTAPE are cylinders. Hartmanis and Berman used the existence of *padding* functions to construct polynomial isomorphisms of all known NP-complete sets. For completeness, we include a treatment of cylinders in a polynomial setting: we begin by establishing the equivalence of having padding functions and being a cylinder.

[2] For a discussion and application of similar structual methods to a variety of other problems involving polynomial reductions among sets in NP, see [26, 27, 10].

[3] We use as the universal set $\mathbb{N}$, which is the set $\{0, 1, 2, \ldots\}$ of natural numbers. By *polynomial* functions or sets we mean polynomial time computable. We take $\langle , \rangle$ to be any of the standard polynomially computable pairing functions bijecting $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$, while Π_1 is its polynomially computable first projection. We assume without further discussion standard properties of such functions; for example, that $\langle 0, 0\rangle = 0$ and that $\langle , \rangle$ is monotone in each argument. By $B \times \mathbb{N}$ we mean the set $\{\langle b, n\rangle : b \in B \text{ and } n \in \mathbb{N}\}$. A more concrete representation as strings might be $\{b \# n : b \in B \text{ and } n \in \mathbb{N}\}$, where $\#$ is a new symbol (see [16] for a discussion of these other representations).

Definition 2.1. A set C is a *cylinder* if C is polynomially isomorphic to $B \times \mathbb{N}$ for some set B.

Definition 2.2. Let C be any set. A *padding function* for C is a one-one, polynomially time computable, polynomial time invertible function p such that, for all x and y, $x \in C$ iff $p(x, y) \in C$.[4] (The idea is that p enables us to quickly produce new elements which, without knowing whether the original element x is in C, preserve membership or nonmembership in C.)

Notation in the paper will be fairly standard, generally following that of [16]. However, from this point on all reducibilities considered will be polynomial time computable, and we will sometimes omit mention of this fact. We will write

$$B \leqslant_{\mathrm{m}} C$$

if there is a *polynomially* computable function f such that $x \in B$ iff $f(x) \in C$. If f can be taken one-one, we write

$$B \leqslant_{1} C.$$

If f can be taken one-one and polynomially invertible, we write

$$B \leqslant_{1,\mathrm{i}} C.$$

If, in addition to all of this, f can be taken to be size increasing (or simply nondecreasing), we write

$$B \leqslant_{1,\mathrm{i}}^{\mathrm{si}} C.$$

If we have both $A \leqslant_{1} B$ and $B \leqslant_{1} A$ we write

$$A \equiv_{1} B.$$

Finally, an even stronger condition than $A \equiv_{1} B$ is that $A \leqslant_{1,\mathrm{i}} B$ by a function f which is both onto and polynomially invertible (so that $B \leqslant_{1,\mathrm{i}} A$ by f^{-1}); in this case, we write

$$A =_{\mathrm{iso}} B,$$

and we say that A and B are *polynomially isomorphic.* Here, of course, to say that f is onto is to say that the range of f is the universal set $\mathbb{N}$.

[4] The definition in [1] only requires that the inverse of $p(x, y)$ yields y instead of yielding $\langle x, y \rangle$. If one chooses, as in [1] to ask for polynomial invertibility only in the second argument, then setting $p'(x, y) = p(x, \langle x, y \rangle)$ gives polynomial invertibility in both arguments. Thus the two definitions are equivalent. We follow the more traditional definition [21]. In a result analogous to Lemma 2.4 below, Berman and Hartmanis [1] require an additional padding function with a strong size-increasing property. The techniques used in the proof of Lemma 2.4 show that the size increasing function is unnecessary. Although Theorem 2.3 establishes the equivalence of the two approaches, our proof may be of independent interest.

Theorem 2.3. (i) *A set C is a cylinder, iff*
(ii) *for every set B, $B \leqslant_m C$ implies $B \leqslant_{1,i} C$, iff*
(iii) $C \times \mathbb{N} \leqslant_{1,i} C$, *iff*
(iv) *C has a padding function.*

This theorem is standard in recursion theory. In a polynomial setting it is perhaps first found in [4]; we include it for completeness. The key to its proof is the following lemma.

Lemma 2.4. *If two sets in the same polynomial many-one degree both have padding functions, then they are polynomially isomorphic.*

Comment. Versions of this lemma for general computable (not just polynomially computable) functions may be found in [21] or [23]. In the polynomial case, it has been used in [1] and in [8], but always using the fact that one could freely assume that one of the padding functions be not too rapidly decreasing in its second argument. Our proof requires no such restriction. Hence, it is more direct, and it may be useful in situations where no such assumption is possible.

Proof of Lemma 2.4. Assume that we have sets A and B with polynomial functions f, reducing A to B, and g, reducing B to A. Assume further that we have padding functions p_A, for A, and p_B, for B. We then define reductions f_1 and g_1 as follows:

$$f_1(y) = \begin{cases} p_B(f(y), p_A(p_A(x, z), 2w)) & \text{if } y = p_A(x, p_A(z, w)), \\ p_B(f(y), p_A(y, 2y+1)) & \text{otherwise;} \end{cases}$$

$$g_1(y) = \begin{cases} p_A(g(y), p_A(p_A(x, z), 2w)) & \text{if } y = p_B(x, p_A(x, w)), \\ p_A(g(y), p_A(y, 2y+1)) & \text{otherwise.} \end{cases}$$

Obviously, f_1 and g_1 are polynomially computable, one-one, and reductions of A to B and of B to A. Furthermore, since both p_A and p_B are polynomially invertible, so are f_1 and g_1. The critical observation to make, however, is that if u is in the range of f_1, then u is of the form $p_B(s, p_A(t, w))$, while if u is in the range of g_1, then u is of the form $p_A(s, p_A(t, w))$. But g_1 applied to any u of the first form increases w to $2w$, while f_1 applied to any u of the second form increases w to $2w$. It follows that if we start with any u in the range of g_1 and successively calculate $g_1^{-1}(u), f_1^{-1}g_1^{-1}(u), \ldots$, then at most $\log_2(w)$ calculations can be made, and hence the time for the calculation is polynomial in u. Thus we may define a polynomially computable, polynomially invertible isomorphism, τ, mapping A to B in the conventional way (see, e.g., [16, pp. 114 ff.] or [1]): given u, calculate $g_1^{-1}(u), f_1^{-1}g_1^{-1}(u), \ldots$ as long as possible; if the last calculation possible is a calculation of f_1^{-1}, then $\tau(u) = f_1(u)$; if the last calculation possible is a calculation of g_1^{-1}, then $\tau(u) = g_1^{-1}(u)$. It is easily verified that τ is the desired polynomial-time isomorphism between A and B. □

Proof of Theorem 2.3. (i)⇒(ii): Suppose that $C \equiv_{iso} D \times \mathbb{N}$ for some set D. Clearly, if $B \leq_m C$, then $B \leq_m D \times \mathbb{N}$ by some function g. Since $g'(x) =_{def} \langle \Pi_1(g(x)), x \rangle$ gives an obvious $\leq_{1,i}$-reduction of B to $D \times \mathbb{N}$, the isomorphism between $D \times \mathbb{N}$ and C now yields $B \leq_{1,i} C$. Thus $B \leq_m C$ implies $B \leq_{1,i} C$.

(ii)⇒(iii): Since $C \times N \leq_m C$, from (ii) we have that $C \times \mathbb{N} \leq_{1,i} C$.

(iii)⇒(iv): We now have $C \leq_{1,i} C \times \mathbb{N} \leq_{1,i} C$; by using the obvious compositions, the padding function on $C \times \mathbb{N}$ induces a padding function on C.

(iv)⇒(i): Since C and $C \times \mathbb{N}$ are obviously in the same many-one degree and since $C \times \mathbb{N}$ obviously has a padding function, it follows that if C also has a padding function, Lemma 2.4 guarantees that $C =_{iso} C \times \mathbb{N}$. The latter condition in turn establishes by definition that C is a cylinder, completing our circle of equivalences and the proof of the theorem.[5] □

Sets which are cylinders have very uniform and fast methods of generating members of both the set and its complement. Sets which have no method of quickly generating (and inverting) *some* subset of the set will be called *immune.*

Definition 2.5. A set I is (polynomially) *immune* if there does not exist a one-one polynomially computable, polynomially *invertible*, function p such that *range p* is contained in I. If there does not exist a one-one polynomially computable function p such that *range p* is contained in I, then we will call I *strongly immune.*[6,7]

3. Constructions of non-isomorphic sets

It follows from Theorem 2.3 that if a many-one degree does not consist of a single isomorphism type, then it contains a set S which is not a cylinder. Thus both S and $S \times \mathbb{N}$ are in this same many-one degree, $S \leq_{1,i} S \times \mathbb{N}$, but $S \times \mathbb{N} \not\leq_{1,i} S$.

The outline of this section is: First, that for sets like S and $S \times \mathbb{N}$ we can establish a *finite difference property*: finite variants of $S \times \mathbb{N}$ will not be $\not\leq_{1,i}$-reducible to finite variants of S. Second, that the finite difference property permits a *delayed diagonalization* construction of incomparable sets C and D that are strictly between S and $S \times \mathbb{N}$ under the ordering of $\leq_{1,i}$. Finally, we show that the new sets C and D *inherit* suitable properties which guarantee the finite difference property, allowing us to repeat the construction.

[5] If we do not demand that padding functions be polynomially invertible, then Theorem 2.3 holds with $\leq_{1,i}$ replaced by $\leq_1$ and with $=_{iso}$ replaced by $\equiv_1$. A similar remark holds for all of the other results and definitions of this paper as well. The proofs are essentially the same, although simpler.

[6] Note that the definition of polynomial immunity we use here is different from that of Ko and Moore [11], and different also from notions of immunity discussed in [10].

[7] It is known that if P ≠ NP, then no NP-complete set can have a *sparse* complement [2, 5], and, more significantly [18], no NP-complete set can be *sparse.* However, while all sparse sets are immune, the converse is false. Indeed, Ladner's construction [13] can be used to show that if P ≠ NP, then there are strongly immune, strongly co-immune, sets in NP − P which are not sparse. Sets in NP with immune complements might be called *simple.* The existence in the presence of oracles of various types of sparse/simple sets is investigated in [9, 12].

There are two deviations from this outline: the major problem is that it is not easy to establish the inheritance of the finite difference property for the constructed sets, C and D. We postpone a proof of this property in the generality we require until Section 4; the proof given there is long and the reader may choose to omit reading it. Nevertheless, we will state and use the finite difference result in this section. The second deviation we address immediately:

We will construct sets which are not polynomially isomorphic to S or $S \times \mathbb{N}$, but which are many-one equivalent to S. In constructing a reduction of S to the new set we will need to map certain elements away from the elements that were used in the diagonalization. Also, to establish the hereditary finite difference properties, we need to map certain elements away from finite sets. Both of these requirements can be satisfied by a non-immunity property for $\bar{S}$. In [17], this is solved by first showing that the complements of either $S \times \{0\}$ or $\bar{S} \times \{0\}$ will permit constructing the needed reductions; and second that one of those sets is not polynomially isomorphic to a cylinder (proved by R. Cole in [17]). (No hereditary properties are established there.) Our construction here is similar, but we use precisely a non-immunity property to construct reductions and to establish the hereditary properties. Our proof gives a slightly stronger result than is found in [17].

Theorem 3.1. *Let S be any set. Define S_0 to be $S \times \{0\}$, and define S_1 to be $(S \times \{0\}) \cup (\mathbb{N} \times (\mathbb{N} - \{0\}))$ or, more simply, define $\overline{S_1}$ to be $\bar{S} \times \{0\}$. (Pictures of S_0 and of S_1 may be helpful.) Then S is a cylinder iff both S_0 and S_1 are cylinders.*

Comment. Cole's result in [17] states that for any set S, if both S_0 and S_1 are cylinders, then S is a cylinder. Examination of our *proof*, however, shows that we have a stronger theorem than we have stated: in the reverse direction, our proof really shows that if *either* S_0 is a cylinder and $\bar{S}_1$ is not immune *or* S_1 is a cylinder and S_0 is not immune, then S is a cylinder. In discussing Cole's result, Mahaney [17] conjectures that this result really is not necessary (when $S \times \mathbb{N}$ is polynomially isomorphic to SAT) because he conjectures that if $\mathrm{SAT} \equiv_m S$ and $\mathrm{SAT} \not\leq_{1,i} S$, then $\mathrm{SAT} \not\leq_{1,i} S_0$. Our (strengthened) theorem sheds some light on this conjecture: If one could extend the result of Fortune [5] to show that no set which is Karp-complete for NP can be simple, then Mahaney's conjecture would follow from our stronger theorem. Of course, in recursive function theory, the result that no many-one complete r.e. set can be simple is a cornerstone of the whole structural approach [20]. (Similar remarks apply to the set S_1 if one could strengthen the result of [18] showing that no NP-complete set can be sparse to show that no Karp-complete set can be immune.)

Proof of Theorem 3.1. First suppose that S is a cylinder with padding function p. Define p' by

$$p'(\langle x, 0\rangle, z) = \langle p(x, z), 0\rangle, \qquad p'(\langle x, y+1\rangle, z) = \langle x, \langle y+1, z\rangle\rangle.$$

Clearly p' is a padding function for both S_0 and S_1.

Now suppose that S_0 and S_1 are both cylinders. The fact that S_1 is a cylinder implies that $\bar{S} \times \{0\}$ is not immune. Let p be a polynomially computable, polynomially invertible function such that *range* p is a subset of $\bar{S} \times \{0\}$. Let p_0 be a padding function for $S \times \{0\}$. We define a padding function p_S for S by

$$p_S(x, y) = \begin{cases} \Pi_1(p_0(\langle x, 0\rangle, y)) & \text{if } p_0(\langle x, 0\rangle, y) \in (\mathbb{N} \times \{0\}) - (\textit{range } p), \\ \Pi_1(p(\langle x, y\rangle)) & \text{otherwise.} \end{cases}$$

Elementary calculations then show that p_S is a padding function for S. □

We have now progressed to the following point: Suppose that we have a many-one degree that does not consist of a single isomorphism type. Then there is a set S in the many-one degree which is not a cylinder and, letting $S_4 = S \times \mathbb{N}$, either Condition A or Condition B below obtains.

Condition A (S_0 is not a cylinder)

(i) $S_0 \subseteq S_4$ *and* $S_4 - S_0$ *is infinite,*

(ii) $S_4 \not\leq_{1,i} S_0$,

(iii) $S_0 \leq^{si}_{1,i} S_4$,

(iv) $S_0 = (S_4 \cap P_0)$ *for some polynomially decidable set* P_0, *and*

(v) $\bar{S}_4$ *is not immune.*

(*Take* $p(n) =_{def} \langle i_1, n\rangle$ *for some* i_1 *in* $\bar{S}$. *Note also that* p *is size-increasing.*)

Condition B (S_1 is not a cylinder). (This is similar to Condition A with S_1 substituted for S_0 and $\bar{S}_4$ substituted for S_4.)

(i) $S_1 \subseteq \bar{S}_4$ *and* $\bar{S}_4 - S_1$ *is infinite,*

(ii) $\bar{S}_4 \not\leq_{1,i} S_1$,

(iii) $S_1 \leq^{si}_{1,i} \bar{S}_4$,

(iv) $S_1 = (\bar{S}_4 \cap P_1)$ *for some polynomially decidable set* P_1, *and*

(v) S_4 *is not immune.*

(*Take* $p(n) =_{def} \langle i_0, n\rangle$ *for some* i_0 *in* S. *Note also that* p *is size-increasing.*)

Henceforth, we will assume that Condition A holds; our constructions in case Condition B holds will be entirely similar.

The finite difference property is that if $A \not\leq_{1,i} B$, then finite variants of A will not be $\leq_{1,i}$-reducible to finite variants of B. The property is used to guarantee the existence of appropriate witnesses in the delayed diagonalization construction which we shall give later. Since this finite difference property is not generally valid, we need to derive conditions on A and B which guarantee its validity. Conditions A and B above turn out to be sufficient for this purpose, but the proof is difficult, so we merely state the necessary theorem here, delaying its full proof until Section 4 of this paper. For motivation, however, we will prove the finite variant condition under the assumption that the set B (the set S_4 in Conditions A and B) is a polynomial cylinder. We now state the finite variant condition.

Theorem 3.2. *Assume S_0 and S_4 satisfy Condition A. Let F_4 and F_0 be any two finite sets. Suppose that $g: S_4 - F_4 \leq_1 S_0 \cup F_0$. Then there is a function g' such that $g': S_4 \leq_1 S_0$. Furthermore, if g is polynomially invertible, so is g'. If g is size-increasing so is g'. Thus, there can be no $\leq_{1,i}$-reduction of $S_4 - F_4$ to $S_0 \cup F_0$. A similar result holds for S_1 and $\bar{S}_4$ if Condition* B *holds.*

Proof. We defer a proof of this result until the next section, but for motivation we include here a proof for Condition A under the additional assumption that S_4 is a polynomial cylinder. Under these assumptions, consider the finite set F of elements of S_4 that are either in F_4 or map into F_0 by g. Let $s \in S_4$ be larger than any element in F. The elements of F should be mapped into S_0; the membership of other elements is properly preserved by g. A padding function $p(,)$ for S_4 easily permits moving elements out of the way. We may choose p to be size-increasing since S_4 is a cylinder. Now define

$$g'(x) = \begin{cases} g(p(x, 0)) & \text{if } x \notin F, \\ g(p(s, x+1)) & \text{if } x \in F. \end{cases}$$

Then $g': S_4 \leq_1 S_0$. If g is size increasing or invertible then g' is also. □

Theorem 3.3 is really a corollary of the more general Theorem 3.4, which follows below. However, by first proving Theorem 3.3 carefully it will be evident how to prove the more general result, and we will then merely outline the proof of the more general theorem which follows.

Theorem 3.3. *Every polynomial many-one degree which does not consist of a single isomorphism type contains sets which are incomparable under $\leq_{1,i}$. Every polynomial many-one degree which does not consist of a single isomorphism type contains a collection of isomorphism types which have order type of the rationals under $\leq_{1,i}^{si}$.*

Proof. We know that if we have a many-one degree which does not consist of a single isomorphism type, then there are sets S_0, S_1, and S_4 such that either Condition A or Condition B above obtains. We will assume Condition A in our discussion; the argument for Condition B is similar.

Our goal is to describe $\leq_{1,i}$-incomparable sets S_2 and S_3 such that each of them lies between S_0 and S_4 under $\leq_{1,i}$-reductions. (In fact, even under $\leq_{1,i}^{si}$-reductions.) Furthermore, for both $j = 2$ and 3, we want Condition A to hold, first with S_j substituted for S_4, and then with S_j substituted for S_0. If we can accomplish this, then Condition A will be 'hereditary' for the sets we describe, and thus our construction can be repeated indefinitely, first between S_0 and S_2 or S_3 and then between S_2 or S_3 and S_4, yielding the required dense linear orderings.

(Note that if we only have the weaker version of Theorem 3.2 which requires that the set S_4 be a polynomial cylinder, then the finite variant condition is not hereditary between S_0 and S_2 nor between S_0 and S_3. In this case, the construction can be

repeated only between S_2 or S_3 and S_4, and this yields orderings only of type $\omega+1$ under $\leqslant^{si}_{1,i}$. This is the chief reason why Mahaney [17] established orderings of type $\omega+1$, rather than the more general orderings which we establish here.)

Now, to actually do the construction, we will need to establish incomparability under $\leqslant_{1,i}$-reductions, and we will require an explicit indexing f_i of reductions; further let

$$t_k = \langle f_a, f_b, c+n^c \rangle$$

be an indexing of triples so that every combination of f_a, f_b, and polynomial $c+n^c$ appears in some triple t_k. Each triple is considered as a candidate for a reduction, its inverse, and a polynomial time bound for both reductions.

In order to establish that $S_2 \not\leqslant_{1,i} S_3$, for each t_k we will witness that t_k is not such a reduction. The witnesses show

(i) f_a is not a reduction of S_2 to S_3, or
(ii) f_a is not one-one, or
(iii) f_b is not inverse to f_a, or
(iv) one of the functions uses more than $c+n^c$ steps.

Each witness is an element or two; for example, to witness that f_a is not one-one, two elements x and y such that $f_a(x)=f_a(y)$ are needed. To witness that $S_3 \not\leqslant_{1,i} S_2$, we interchange the roles of S_2 and S_3.

Our construction will proceed in alternating stages. The stages define two polynomially recognizable sets P_2 and P_3, and we will define

$$S_2 = (S_4 \cap P_2) \quad \text{and} \quad S_3 = (S_4 \cap P_3).$$

Since for $j=2,3$ we will make $P_0 \subset P_j$, we will have $S_0 \subset S_j \subset S_4$. During any stage we will have that each S_j is S_0 plus a subset of S_4. To accomplish this, during each stage we begin in a polynomial fashion to add all elements of P_0 both to P_2 and to P_3. (I.e., we are adding all elements of S_0 to both S_2 and to S_3.) We maintain these sets so that $S_2 \cap S_3 = S_0$ (by maintaining $P_2 \cap P_3 = P_0$).

During stage $2k$ we will have that S_3 is S_0 plus a finite subset of S_4. During this stage we add elements to P_2 (and thus to S_2) until witnesses are found that t_k is not an $\leqslant_{1,i}$-reduction of S_2 to S_3. We are assured that such elements exist by Theorem 3.2. For if no such witnesses exist, then we will put all but finitely many elements of S_4 into S_2, and have

$$S_4 - ((S_4 - S_0) \cap P_3) = S_2 \leqslant_{1,i} S_3 = S_0 \cup ((S_4 - S_0) \cap P_3).$$

Since $((S_4 - S_0) \cap P_3)$ is finite, this gives the hypothesis of Theorem 3.2(i). The conclusion that $S_4 \leqslant_{1,i} S_0$ contradicts the hypothesis of this theorem. We conclude, therefore, that the witnesses will exist and will halt stage $2k$ after a finite number of additions to P_0. In the stage $2k+1$ the roles of S_2 and S_3 are reversed.

We construct these polynomially decidable sets P_2 and P_3 by using a 'delayed diagonalization' [3, 13]. Our construction determines whether elements are in P_2 or

P_3. Let $q(\ )$ be some arbitrary polynomial (chosen to bound the running time of certain operations in this procedure).

On input n, simulate this construction on 0, 1, 2, ..., i for exactly $q(|n|)$ steps (note the implicit recursion). By counting the alternations between assigning elements to P_2 and P_3, we can determine that the simulation on element i was in stage $2k$ or $2k+1$ for some k.

At stage $2k$ we search among $0, 1, 2, \ldots$ using at most $q(|n|)$ steps to see if we find a witness to the fact that, if we let $S_2 = (P_0 \cup P_2) \cap S_4$ and if we let $S_3 = (P_0 \cup P_3) \cap S_4$, then the triple t_k does not yield $S_2 \leq_{1,i} S_3$. If no such witness is found, we assign the input n to P_2. Otherwise, we assign it to P_3.

At stage $2k+1$ we simply reverse the roles, searching until we get a witness to the fact that if we let S_2 and S_3 be defined as above, then the triple t_k does not yield $S_3 \leq_{1,i} S_2$. If no such witness is found, we assign the input to P_3, otherwise to P_2.

Note that we have implicitly described a recursion whose running time is polynomial in the size of the input.

Obviously, neither of the sets S_2 and S_3 can be reduced to the other via a polynomially computable, polynomially invertible, one-one function.

The function f defined by

$$f(x) = \begin{cases} x & \text{if } x \in P_0, \\ p(x) & \text{otherwise,} \end{cases}$$

clearly demonstrates both $S_0 \leq^{\text{si}}_{1,i} S_2$ and $S_0 \leq^{\text{si}}_{1,i} S_3$.

The functions f_j defined by

$$f_j(x) = \begin{cases} x & \text{if } x \in P_0 \cup P_j, \\ p(x) & \text{otherwise,} \end{cases}$$

demonstrates that $S_j \leq^{\text{si}}_{1,i} S_4$ for each of $j = 2$ or 3.[8]

Obviously, because S_2 and S_3 are incomparable under $\leq_{1,i}$, we cannot have either $S_4 \leq_{1,i} S_2$ or $S_4 \leq_{1,i} S_3$. For the same reason, we cannot have either $S_2 \leq_{1,i} S_0$ or $S_3 \leq_{1,i} S_0$. We thus have that S_2 and S_3 each lie strictly between S_0 and S_4 (even under strictly size increasing reductions). Since it is also obvious from the construction that Condition A now holds again with either of S_2 or S_3 replacing either of S_0 or S_4 in statement, Condition A is *hereditary* for the construction, and so the construction may be repeated for either of $j = 1, 2$, first to place sets between S_0 and S_j, and then to place sets between S_j and S_4. Repeating this procedure clearly produces dense linear orderings.

[8] The ease of *these* reductions is another major difference between the proof given here and the proof in [17] that many-one degrees which contain more than one isomorphism type contain infinitely many with ordering $\omega + 1$. Both proofs incorporate a delay to switch stages, but the proof in [17] required a more delicate alternation of stages to establish the existence of reductions similar to these. This further delay, while not necessary for our proof, may be useful in other applications using 'delayed diagonalization'.

The proof when Condition B rather than Condition A holds for the many-one degree is essentially the same. We use S_1 for S_0 and $\bar{S}_4$ for S_4. Thus the proof of the theorem is complete. □

Theorem 3.3 is now easily generalized to the following theorem.

Theorem 3.4. *Any polynomial many-one degree which fails to consist of a single isomorphism type contains every possible countable linear ordering under the ordering* $\leqslant_{1,i}^{si}$. *The incomparable sets in the ordering are incomparable even under* $\leqslant_{1,i}$.

Proof. We begin with the observation that Mostowski [19] has given a recursive partial order which is *universal* in the sense that every countable partial order can be embedded in it.[9] We begin with our sets S_0 and S_4 as in Condition A, and with an enumeration of the edges in a universal ordering. At stage k we do all of the following: find all of the vertices which have appeared in the listing to date. (To keep things simple, if we wish, we can slow down the appearance of vertices and edges so that at most $\log k$ vertices and edges have appeared by stage k.) We will say that $y \leqslant z$ *has appeared* if enough edges have appeared in the enumeration of the edges to show that $y \leqslant z$ in the ordering. For each vertex y which has appeared let

$$A_y = \{z \mid y \leqslant z \text{ has appeared}\}.$$

For each x *not* in A_y and for each z in A_y, begin adding elements of S_4 to S_z until we get witnesses that the triple t_k is not a one-one polynomial invertible reduction of S_z to the set S_x. Since at this point each of the sets S_x differs only finitely from S_0 while if the process continues each S_z will differ only finitely from S_4, we know by Theorem 3.2 that this process cannot continue indefinitely.

The above process shows directly that if we do not eventually get $x \leqslant z$ (implicitly) enumerated in the universal ordering, then for each k we must have that t_k does not give a $\leqslant_{1,i}$-reduction of S_z to S_x. On the other hand, once in the ordering we discover that $y \leqslant z$, then we force $S_y \subseteq S_z$ except for the finite set of points already in S_y. Since, for all y, $S_y = S_4 \cap P_y$ where P_y is *the* polynomial set described implicitly in the construction above, obviously the same reduction (constructed exactly as in the proof of Theorem 3.3) which witnesses that $S_y \leqslant_{1,i}^{si} S_4$ witnesses that $S_y \leqslant_{1,i}^{si} S_z$

[9] We are grateful to Rick Statman for pointing out Mostowski's paper to us and, on seeing our proof of Theorem 3.2, suggesting that Theorem 3.3 should be obtainable by combining our techniques with Mostowski's result. He also pointed out that the existence of recursively enumerable universal partial orders was used earlier by Sacks [22] in investigating degree structures of Turing reducibilities. In using this result in [14], Machtey showed that the ordering could be made primitive recursive, and, again in [15], he showed that the ordering can be made elementary. Statman, however, has observed that the construction orginally given by Mostowski produces a very nice *polynomial* ordering for which, given two vertices, one can decide in polynomial time whether there is an edge from one to the other. However for our purposes all we need is the existence of a universal partial ordering in which the edge structure is merely recursively enumerable.

except on the finitely many elements of S_y which do not belong to S_z. But since $S_z - S_x$ is infinite, and none of these elements are in the range of the above reduction, there is plenty of room in $S_z - S_y$ to place these finitely many elements, yielding $S_y \leq^{si}_{1,i} S_z$.

The case where we start with the sets S_1 and S_4 is entirely similar, proving the theorem. □

Note that, in this proof, we do not need the 'hereditary' aspects of the proof of Theorem 3.2 since we have collapsed the construction of all the of the necessary sets into one large, essentially simultaneous, construction. In particular, this means that, unlike the proof we gave for Theorem 3.3, the proof just given for the more general Theorem 3.4 does not require the full force of Theorem 3.2. We have used only that portion of Theorem 3.2 already proven, in which we assumed that the set S_4 is a cylinder.

Corollary 3.5. *The class* P^- *of nontrivial sets decidable in polynomial time has many-one degree whose isomorphism types contain every possible countable partial order under* $\leq_{1,i}$*-reductions. If the class* NP − P *is nonempty, then it contains similar many-one degrees.*

Proof. As already remarked in earlier footnotes, Ladner's technique of delayed diagonalization easily shows that, when nonempty, each of these classes contains sets which are polynomially immune and hence cannot be polynomial cylinders. The result is then immediate. □

4. The full theorem on finite differences

This section gives the full proof of Theorem 3.2, which we needed only for the proof we gave of Theorem 3.3. In spite of the fact that the full proof of Theorem 3.2 is not needed to establish our most general results above, its correctness served as a powerful motivation for both proofs given above. Furthermore, should one wish to insert any sort of orderings between sets S_0 and S_4 where it is known that $S_0 \leq_1 S_4$ but it is not known a priori that S_4 is a cylinder, then some version of Theorem 3.2 appears to be essential.

Recall that we are given three sets S_0, S_1, and S_4 satisfying one of Conditions A and B of Section 3.

(In the applications given above the *origin* of these sets is either

(a) that we have a many-one degree that does not consist of a single isomorphism type. Then there is a set S in the many-one degree which is not a cylinder and, we let $S_0 = S \times 0$, $S_1 = S \times \mathbb{N} \cup \mathbb{N} \times (\mathbb{N} - \{0\})$, and $S_4 = S \times \mathbb{N}$.

Or else

(b) that the three sets are constructed hereditarily from the sets given in (a) as in the proof of Theorem 3.3.

In the first case, the four parts of each of the conditions are obvious, and, in the second case, as we have already pointed out, the construction guarantees the four parts.)

We are now ready to prove the key theorem on finite differences. Simple as this theorem is, and obvious as it should be, the proof which we give uses all of the many parts of Conditions A and B. As we have seen, once established, the theorem has served to provide a relatively simple proof of Theorem 3.3, and it served as well to help motivate Theorem 3.4. We now repeat the statement of Theorem 3.2, and give its complete proof.

Theorem 3.2. (i) *Let S_4 and S_0 be two sets satisfying Condition* A, *and let F_4 and F_0 be any two finite sets. Suppose that $g: S_4 - F_4 \leq_1 S_0 \cup F_0$. Then there is a function g' such that $g': S_4 \leq_1 S_0$. Furthermore, if g is polynomially invertible so is g'. If g is size-increasing, so is g'.*

(ii) *Let S_4 and S_1 be two sets satisfying Condition* B, *and let F_4 and F_1 be any two finite sets. Suppose that $g: \bar{S}_4 - F_4 \leq_1 S_1 \cup F_1$. Then there is a function g' such that $g': \bar{S}_4 \leq_1 S_1$. Furthermore, if g is polynomially invertible, so is g'. If g is size-increasing, so is g'.*

Comment. An even stronger theorem would involve, for Condition A, four finite sets, F_0, F_0', F_4, and F_4', with a hypothesis that

$$(S_4 - F_4) \cup F_4' \leq_1 (S_0 \cup F_0) - F_4',$$

and with a similar hypothesis for Condition B. The conclusions of Theorem 3.2 parts (i) and (ii) would still hold. However, we used only the stated version of Theorem 3.2 in our proof of Theorem 3.3, and the reader who struggles through the details of the proof we are about to give will not only be convinced that essentially the same proof will work to prove this stronger theorem, but no doubt also will be grateful that we have not included the necessary details for this stronger theorem.

Proof of Theorem 3.2(i). We give the proof of part (i) along with some motivation; the proof of part (ii) is identical. We begin by making some observations. First, without loss of generality we can assume that $F_4 \subset S_4$, that F_0 is disjoint from S_0, and that F_0 is disjoint from *range p*. Fig. 1 illustrates these relationships. We assume that we have a reduction g of $S_4 - F_4$ to $S_0 \cup F_0$ and that we want to somehow turn g into a similar reduction g' of S_4 to S_0, to produce a contradiction (assuming that g is one-one and polynomially invertible).

Reasoning informally, observe that, except for a finite set, g itself is a solution to the problem; the elements where g is unsuitable are

$$x : x \in F_4,$$

for these points $g(x) \notin S_0$, but we want $g'(x) \in S_0$; and

$$x : g(x) \in F_0,$$

for these points $x \in S_4$, but we want $g'(x) \in S_0$.

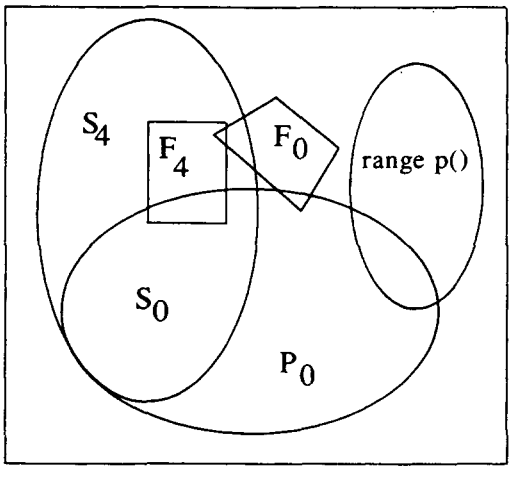

Fig. 1. Hypothesis of Theorem 3.2, condition (i).

It would be a simple matter to define g' if we had sufficient 'space' in $S_0 - g(S_4)$. If we had sufficient space there, we could use g except on the finite set of points mentioned above, and they could then be mapped one-one to the 'extra' space.

Our proof now proceeds in two steps. First we define $\bar{g}$ to give infinite space in $g(S_4) - \bar{g}(S_4) \subset S_0$ under the assumption that F_0 and F_4 are empty. This construction is the main innovation in the proof. Second, we tediously characterize the finite set on which $\bar{g}$ is not a $\leqslant_1$-reduction of S_4 to S_0, and note that these points must reduce to S_0. Then for a suitable finite set F in $S_4 - S_0$ we can define $g'(x) = g(y)$ for y chosen from F.

We assume for the moment that F_0 and F_4 are empty and define $\bar{g}$ to create infinite space in $S_0 - \bar{g}(S_4)$. We will use g^2 to create extra space. We have

$$g(S_4) \subset S_0 \subset S_4,$$

so,

$$g^2(S_4) \subset g(S_0) \subset g(S_4) \subset S_0,$$

and since $S_4 - S_0$ is infinite and g is one-one, we have $g(S_4) - g(S_0)$ is infinite. From the second line of inclusions, it follows that $g(S_4) - g^2(S_4)$ is infinite.

Now note that, outside S_4, g^2 may not behave so nicely; i.e., we may have $x \notin S_4$, $g(x) \in S_4$, and $g^2(x) \in S_0$ (which violates reducing S_4 to S_0). We use P_0, which is polynomial recognizable, to detect such cases (since $g(x) \in S_4 - S_0$ implies $g(x) \notin P_0$), and we use $p(x)$ to place them safely away from S_0. Since $P_0 \cap \textit{range}\, p$ may not be empty, we avoid violating one-oneness there by checking if $g^2(x) \in \textit{range}\, p$.

Thus, we define

$$\bar{g}(x) = \begin{cases} p(x) & \text{if } g(x) \notin P_0 \text{ or } g^2(x) \in \textit{range}\, p, \\ g^2(x) & \text{otherwise.} \end{cases}$$

The argument above establishes that $g(S_4) - \bar{g}(S_4)$ is infinite and that $\bar{g}$: $S_4 \leqslant_1 S_0$. If g is invertible or size-increasing, then so is $\bar{g}$.

We now proceed with the second step, considering that F_0 and F_4 may not be empty. First note that this introduces only finite many exceptions to our assertion that $\bar{g}$: $S_4 \leq_1 S_0$; further, this finite set of exceptions cannot deplete the infinite space in $g(S_4) - S_4$ very much. We complete our proof by characterizing the exceptions, and then defining g' to be $\bar{g}$ except on the exceptions, which we then send to the infinite space.

First we consider the condition:

$\alpha(x)$: $x \in F_4$ or $g(x) \in F_0$ or $g(x) \in (F_4 \cap P_0)$.

By examination we see in all three of these cases that we need $g'(x) \in S_0$, but in the first two of these cases we have a problem since $g(x) \notin S_0$. Of course, for any x, if $\alpha(x)$ occurs, we can easily recognize this fact. We begin by letting F be a finite subset of $S_4 - S_0$ such that $g(F) \subset S_0$, all members of F are bigger than all members of $F_0 \cup F_4$, and $|F| \geq 2^*|F_0| + 2^*|F_4|$.

We next observe that if $\alpha(x)$ fails to hold and if $g(x) \notin P_0$, then $x \notin S_4$, so we may simply define $g'(x) = p(x)$.

Since we already known where to map x if $\alpha(x)$ holds, we may now confine our attention to the case where $\alpha(x)$ fails while at the same time $g(x) \in P_0$. But when this occurs we have:

$$x \in S_4 \text{ iff } g(x) \in S_0 \text{ iff } g(x) \in (S_0 - F_4)$$

$$\text{iff } g(x) \in (S_4 - F_4) \text{ iff } g^2(x) \in (S_0 \cup F_0).$$

This suggests one more critical finite condition, namely

$\beta(x)$: $g^2(x) \in F_0$.

Thus if $\alpha(x)$ and $\beta(x)$ *both fail* to hold and if $g(x) \in P_0$ and if $g^2(x) \notin$ *range* p, then we may define $g'(x) = g^2(x)$; while, if $\alpha(x)$ and $\beta(x)$ both fail and if $g(x) \in P_0$ and $g^2(x) \in$ *range* p, then we may define $g'(x) = p(x)$. This leaves only two finite cases remaining. Namely, our earlier case when $\alpha(x)$ holds and the last remaining case when $\beta(x)$ holds while $g(x) \in P_0$ (i.e., when $g^2(x) \in F_0$ while $g(x) \in P_0$).

So far it is easy to see that for all of the x for which we have defined g' if g is one-one and reduces $S_4 - F_4$ to $S_0 \cup F_0$, then g' is one-one and reduces S_4 to S_0. Furthermore, if g is invertible or size-increasing, so is g'. We are now ready to face the problem of the remaining cases, namely, what to do if $\alpha(x)$ or if $\beta(x)$ holds while $g(x) \in P_0$. We have already observed that if $\alpha(x)$ holds, then we need to map x into S_0. In the remaining case, $g^2(x) \in F_0$ guarantees that $g(x) \in (S_4 - F_4)$, so $g(x) \in P_0$ now also guarantees that $g(x) \in S_0$ which in turn guarantees that $x \in S_4$. Thus, just as in case $\alpha(x)$, we must in this last case map x into S_0. Since there are at most $|F_0|$ elements satisfying β and at most $|F_0| + 2^*|F_4|$ elements satisfying α, recalling that $g(F) \subset S_0$, we can take each of the elements x for these remaining cases and define $g'(x) = g(y)$ for some suitable $y \in F$. Since F is finite and reasonably chosen, we can clearly keep g' size-increasing, one-one, and invertible for these particular values of x.

We must still verify that there is no conflict with our earlier chosen values, violating our requirement that g' be one-one. But we now see that for x satisfying α or β, we mapped x into our 'extra' space in S_0: The only conflict could occur if we had $g(y) = g^2(x)$ for some $g(x) \in P_0$. But since g is one-one and $y \notin S_0$, this would yield the contradiction $y = g(x)$.

We leave it to the reader to work out a formal definition of g'. The analysis if Condition B obtains (to prove part (ii) of the theorem) is the same, so we omit it.

Thus, the proof of Theorem 3.2 is complete. □

References

[1] L. Berman and J. Hartmanis, On isomorphism and density of NP and other complete sets, *SIAM J. Comput.* **6** (1977) 305–322.

[2] P. Berman, Relationship between density and deterministic complexity of NP-complete languages, in: *5th Internat. Coll. on Automata, Languages, and Programming*, Lecture Notes in Computer Science **62** (Springer, Berlin, 1978) 63–71.

[3] A. Borodin, R. Constable and J. E. Hopcroft, Dense and nondense families of complexity classes, *IEEE Proc. 10th Ann. Symp. on Switching and Automata Theory* (1969) 7–19.

[4] M. Dowd, On isomorphism, Unpublished manuscript, 1978.

[5] S. Fortune, A note on sparse complete sets, *SIAM J. Comput.* **6** (1979) 431–433.

[6] J. Hartmanis, On log-tape isomorphisms of complete sets, *Theoret. Comput. Sci.* **7** (1978) 273–286.

[7] J. Hartmanis, A note on natural complete sets and Gödel numberings, *Theoret. Comput. Sci.* **17** (1982) 75–89.

[8] J. Hartmanis and T. Baker, On simple Gödel numberings and translations, *SIAM J. Comput.* **4** (1975) 1–11.

[9] S. Homer and W. Maass, Oracle-dependent properties of the lattice of NP sets, *Theoret. Comput. Sci.* **24**(3) (1983) 279–289.

[10] D. Joseph and P. Young, Some remarks on witness functions for nonpolynomial and noncomplete sets in NP, *Theoret. Comput. Sci.* **39**(2, 3) (1985) 225–237 (this issue).

[11] K. Ko and D. Moore, Completeness, approximation and density, *SIAM J. Comput.* **10** (1981) 787–796.

[12] S. Kurtz, On sparse sets in NP−P: Relativizations, *SIAM J. Comput.* **14** (1985) 113–119.

[13] R. Ladner, On the structure of polynomial time reducibility, *J. Assoc. Comput. Mach.* **22** (1975) 155–171.

[14] M. Machtey, The honest subrecursive classes are a lattice, *Inform. & Control* **24** (3) (1974) 247–263.

[15] M. Machtey, On the density of honest subrecursive classes, *J. Comput. System Sci.* **10** (1975) 183–199.

[16] M. Machtey and P. Young, *An Introduction to the General Theory of Algorithms* (Elsevier/North-Holland, New York, 1978).

[17] S. Mahaney, On the number of P-isomorphism classes of NP-complete sets, *Proc. 22nd Ann. IEEE Symp. on Foundations of Computer Science* (1981) 271–278.

[18] S. Mahaney, Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis, *J. Comput. System Sci.* **25** (1982) 130–143.

[19] A. Mostowski, Über gewisse universelle Relationen, *Polskiego Tow Matematycznego* **17** (1938) 117–118.

[20] E. Post, Recursively enumerable sets of positive integers and their decision problems, *Bulletin AMS* **50** (1944) 284–316.

[21] H. Rogers, *Theory of Recursive Functions and Effective Computability* (McGraw-Hill, New York, 1967).

[22] G. Sacks, *Degrees of Unsolvability* (Princeton University Press, Princeton, 2nd ed., 1966).

[23] P. Young, Linear orderings under one-one reducibility, *J. Symbolic Logic* **31** (1966) 70–85.

[24] P. Young, A note on dense and nondense families of complexity classes, *Math. Systems Theory* **5** (1971) 66–70.

[25] P. Young, Some analogues of recursion theoretic results for polynomial reducibilities in NP, *Notices AMS* **3** (1982) 377, Abstract No. 796-68-195.

[26] P. Young, Some structural properties of polynomial reducibilities and sets in NP, *Proc. 15th Ann. ACM Symp. on Theory of Computing* **15** (1983) 392-402.

[27] P. Young, Cook-reducibility is faster than Karp-reducibility by honest functions on NP-complete sets, In preparation.